IP Address Subnetting Tutorial

By Ralph Becker

Ralphb@whoever.com

Updated September 7, 1999

This copy distributed by FirstVPN with author's permission.

Disclaimer

All the information contained in this tutorial is provided for the convenience of its readers. All information is accurate as well as can be reasonably verified. There are no guarantees or warranties stated or implied by the distribution of this information. Use the information in this document at the reader's own risk, and no liability shall be given to the author. Any damage or loss is the sole responsibility of the reader.

Copyright Notice and Distribution Permission

Index

Introduction

IP Addressing

Subnetting

More Restrictive Subnet Masks

An Example

CIDR -- Classless InterDomain Routing

Allowed Class A Subnet and Host IP addresses

Allowed Class B Subnet and Host IP addresses

Allowed Class C Subnet and Host IP addresses

Logical Operations

References and Sources on the Internet

Introduction

This talk will cover the basics of IP addressing and subnetting. Topics covered will include:

- What is an IP Address?
- What are Classes?
- What is a Network Address?
- What are Subnet Masks and Subnet Addresses?
- How are Subnet Masks defined and used?
- How can all this be applied?
- What is CIDR?

IP Addressing

An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points. This is known as "dotted decimal" notation.

Example: 140.179.220.200

It is sometimes useful to view the values in their binary form.

140 .179 .220 .200
10001100.10110011.11011100.11001000

Every IP address consists of two parts, one identifying the network and one identifying the node. The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.

Address Classes

There are 5 different address classes. You can determine which class any IP address is in by examining the first 4 bits of the IP address.

- **Class A** addresses begin with **0xxx**, or **1 to 126** decimal.
- **Class B** addresses begin with **10xx**, or **128 to 191** decimal.
- **Class C** addresses begin with **110x**, or **192 to 223** decimal.
- **Class D** addresses begin with **1110**, or **224 to 239** decimal.
- **Class E** addresses begin with **1111**, or **240 to 254** decimal.

Addresses beginning with **01111111**, or **127** decimal, are reserved for loopback and for internal testing on a local machine. [You can test this: you should always be able to ping **127.0.0.1**, which points to yourself] Class D addresses are reserved for multicasting. Class E addresses are reserved for future use. They

should not be used for host addresses.
Now we can see how the Class determines, by default, which part of the IP address belongs to the network (N) and which part belongs to the node (n).

- Class A -- NNNNNNNN.nnnnnnnn.nnnnnnn.nnnnnnn
- Class B -- NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnnnn
- Class C -- NNNNNNNN.NNNNNNNN.NNNNNNNN.nnnnnnnn

In the example, 140.179.220.200 is a Class B address so by default the Network part of the address (also known as the *Network Address*) is defined by the first two octets (140.179.x.x) and the node part is defined by the last 2 octets (x.x.220.200).

In order to specify the network address for a given IP address, the node section is set to all "0"s. In our example, 140.179.0.0 specifies the network address for 140.179.220.200. When the node section is set to all "1"s, it specifies a broadcast that is sent to all hosts on the network. 140.179.255.255 specifies the example broadcast address. Note that this is true regardless of the length of the node section.

Subnetting

Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

Subnet Masking

Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address* or Number.

For example, using our test IP address and the default Class B subnet mask, we get:

10001100.10110011.11110000.11001000	140.179.240.200	Class B IP Address
11111111.11111111.00000000.00000000	255.255.000.000	Default Class B Subnet Mask
---		
10001100.10110011.00000000.00000000	140.179.000.000	Network Address

Default subnet masks:

- **Class A** - 255.0.0.0 - 11111111.00000000.00000000.00000000
- **Class B** - 255.255.0.0 - 11111111.11111111.00000000.00000000
- **Class C** - 255.255.255.0 - 11111111.11111111.11111111.00000000

More Restrictive Subnet Masks

Additional bits can be added to the default subnet mask for a given Class to further subnet, or break down, a network. When a bitwise logical AND operation is performed between the subnet mask and IP address, the result defines the *Subnet Address*. There are some restrictions on the subnet address. Node addresses of all "0"s and all "1"s are reserved for specifying the local network (when a host does not know it's network address) and all hosts on the network (broadcast address), respectively. This also applies to subnets. A subnet address cannot be all "0"s or all "1"s. This also implies that a 1 bit subnet mask is not allowed. This restriction is required because older standards enforced this restriction. Recent standards that allow use of these subnets have superceded these standards, but many "legacy" devices do not support the newer standards. If you are operating in a controlled environment, such as a lab, you can safely use these restricted subnets.

To calculate the number of subnets or nodes, use the formula (2^n - 2) where n = number of bits in either field. Multiplying the number of subnets by the number of nodes available per subnet gives you the total number of nodes available for your class and subnet mask. Also, note that although subnet masks with non-contiguous mask bits are allowed they are not recommended.

Example:

```
10001100.10110011.11011100.11001000     140.179.220.200  IP Address
11111111.11111111.11100000.00000000     255.255.224.000  Subnet Mask
--------------------------------------------------------
10001100.10110011.11000000.00000000     140.179.192.000  Subnet Address
10001100.10110011.11011111.11111111     140.179.223.255  Broadcast Address
```

In this example a 3 bit subnet mask was used. There are 6 subnets available with this size mask (remember that subnets with all 0's and all 1's are not allowed). Each subnet has 8190 nodes. Each subnet can have nodes assigned to any address between the Subnet address and the Broadcast address. This gives a total of 49,140 nodes for the entire class B address subnetted this way. Notice that this is less than the 65,534 nodes an unsubnetted class B address would have.

Subnetting always reduces the number of possible nodes for a given network. There are complete subnet tables available here for Class A, Class B and Class C. These tables list all the possible subnet masks for each class, along with calculations of the number of networks, nodes and total hosts for each subnet.

An Example

Here is another, more detailed, example. Say you are assigned a Class C network number of 200.133.175.0 (apologies to anyone who may actually own this domain address :). You want to utilize this network across multiple small groups within an organization. You can do this by subnetting that network with a subnet address.

We will break this network into 14 subnets of 14 nodes each. This will limit us to 196 nodes on the network instead of the 254 we would have without subnetting, but gives us the advantages of traffic isolation and security. To accomplish this, we need to use a subnet mask 4 bits long.
Recall that the default Class C subnet mask is

255.255.255.0 (11111111.11111111.11111111.00000000 binary)

Extending this by 4 bits yields a mask of

255.255.255.240 (11111111.11111111.11111111.11110000 binary)

This gives us 16 possible network numbers, 2 of which cannot be used:

Subnet bits	**Network Number**	**Node Addresses**	**Broadcast Address**
0000	200.133.175.0	Reserved	None
0001	200.133.175.16	.17 through .30	200.133.175.31
0010	200.133.175.32	.33 through .46	200.133.175.47

0011	200.133.175.48	.49 through .62	200.133.175.63
0100	200.133.175.64	.65 through .78	200.133.175.79
0101	200.133.175.80	.81 through .94	200.133.175.95
0110	200.133.175.96	.97 through .110	200.133.175.111
0111	200.133.175.112	.113 through .126	200.133.175.127
1000	200.133.175.128	.129 through .142	200.133.175.143
1001	200.133.175.144	.145 through .158	200.133.175.159
1010	200.133.175.160	.161 through .174	200.133.175.175
1011	200.133.175.176	.177 through .190	200.133.175.191
1100	200.133.175.192	.193 through .206	200.133.175.207
1101	200.133.175.208	.209 through .222	200.133.175.223
1110	200.133.175.224	.225 through .238	200.133.175.239
1111	200.133.175.240	Reserved	None

CIDR -- Classless InterDomain Routing

Now that you understand "classful" IP Subnetting principals, you can forget them ;). The reason is **CIDR** -- **C**lassless **I**nter**D**omain **R**outing. CIDR was invented several years ago to keep the Internet from running out of IP addresses. The "classful" system of allocating IP addresses can be very wasteful; anyone who could reasonably show a need for more that 254 host addresses was given a Class B address block of 65533 host addresses. Even more wasteful were companies and organizations that were allocated Class A address blocks, which contain over 16 Million host addresses! Only a tiny percentage of the allocated Class A and Class B address space has ever been actually assigned to a host computer on the Internet.

People realized that addresses could be conserved if the class system was eliminated. By accurately allocating only the amount of address space that was actually needed, the address space crisis could be avoided for many years. This was first proposed in 1992 as a scheme called **Supernetting**. Under supernetting, the classful subnet masks are extended so that a network address and subnet mask could, for example, specify multiple Class C subnets with one address. For example, If I needed about 1000 addresses, I could supernet 4 Class C networks together:

192.60.128.0   Class C subnet address
192.60.129.0   Class C subnet address
192.60.130.0   Class C subnet address
192.60.131.0   Class C subnet address

192.60.128.0   Supernetted Subnet address
255.255.252.0   Subnet Mask
192.60.131.255   Broadcast address

In this example, the subnet 192.60.128.0 includes all the addresses from 192.60.128.0 to 192.60.131.255. The Network portion of the address is 22 bits long, and the host portion is 10 bits long.

Under CIDR, the subnet mask notation is reduced to a simplified shorthand. Instead of spelling out the bits of the subnet mask, it is simply listed as the number of 1s bits that start the mask. In the above example, the network address would be written simply as:

192.60.128.0/22

which indicates starting address of the network, and number of 1s bits in the network portion of the address.

It is currently almost impossible to be allocated IP address blocks. You will simply be told to get them from your ISP. The reason for this is the ever-growing size of the Internet routing table. Just 5 years ago, there were less than 5000 network routes in the entire Internet. Today, there are over 80,000. Using CIDR, ISPs are allocated large chunks of address space (usually with a subnet mask of /19 or even smaller); the ISP's customers are then allocated networks from the ISP's pool. That way, all the ISP's customers are accessible via 1 network route on the Internet. But I digress.

It is expected that CIDR will keep the Internet happily in IP addresses for the next few years at least. After that, IPv6, with 128 bit addresses, will be needed. Under IPv6, even sloppy address allocation would comfortably allow a billion unique IP addresses for every person on earth! The complete and gory details of CIDR are documented in RFC1519, which was released in September of 1993.

Allowed Class A Subnet and Host IP addresses

# bits	Subnet Mask	# Subnets	# Hosts	Nets * Hosts
2	255.192.0.0	2	4194302	8388604
3	255.224.0.0	6	2097150	12582900
4	255.240.0.0	14	1048574	14680036
5	255.248.0.0	30	524286	15728580
6	255.252.0.0	62	262142	16252804
7	255.254.0.0	126	131070	16514820
8	255.255.0.0	254	65534	16645636
9	255.255.128.0	510	32766	16710660
10	255.255.192.0	1022	16382	16742404
11	255.255.224.0	2046	8190	16756740
12	255.255.240.0	4094	4094	16760836
13	255.255.248.0	8190	2046	16756740
14	255.255.252.0	16382	1022	16742404
15	255.255.254.0	32766	510	16710660
16	255.255.255.0	65534	254	16645636

17	255.255.255.128	131070	126	16514820
18	255.255.255.192	262142	62	16252804
19	255.255.255.224	524286	30	15728580
20	255.255.255.240	1048574	14	14680036
21	255.255.255.248	2097150	6	12582900
22	255.255.255.252	4194302	2	8388604

Allowed Class B Subnet and Host IP addresses

# bits	Subnet Mask	# Subnets	# Hosts	Nets * Hosts
2	255.255.192.0	2	16382	32764
3	255.255.224.0	6	8190	49140
4	255.255.240.0	14	4094	57316
5	255.255.248.0	30	2046	61380
6	255.255.252.0	62	1022	63364
7	255.255.254.0	126	510	64260
8	255.255.255.0	254	254	64516
9	255.255.255.128	510	126	64260
10	255.255.255.192	1022	62	63364
11	255.255.255.224	2046	30	61380
12	255.255.255.240	4094	14	57316
13	255.255.255.248	8190	6	49140
14	255.255.255.252	16382	2	32764

Allowed Class C Subnet and Host IP addresses

# bits	Subnet Mask	# Subnets	# Hosts	Nets * Hosts
2	255.255.255.192	2	62	124
3	255.255.255.224	6	30	180
4	255.255.255.240	14	14	196

5	255.255.255.248	30	6	180
6	255.255.255.252	62	2	124

Logical Operations

This page will provide a brief review and explanation of the common logical bitwise operations AND, OR, XOR and NOT. Logical operations are performed between two data bits (except for NOT). Bits can be either "1" or "0", and these operations are essential to performing digital math operations.
In the "truth tables" below, the input bits are in **bold**, and the results are plain.

AND

The logical AND operation compares 2 bits and if they are both "1", then the result is "1", otherwise, the result is "0".

	0	**1**
0	0	0
1	0	1

OR

The logical OR operation compares 2 bits and if either or both bits are "1", then the result is "1", otherwise, the result is "0".

	0	**1**
0	0	1
1	1	1

XOR

The logical XOR (Exclusive OR) operation compares 2 bits and if exactly one of them is "1" (i.e., if they are different values), then the result is "1"; otherwise (if the bits are the same), the result is "0".

	0	**1**
0	0	1
1	1	0

NOT

The logical NOT operation simply changes the value of a single bit. If it is a "1", the result is "0"; if it is a "0", the result is "1". Note that this operation is different in that instead of comparing two bits, it is acting on a single bit.

0	**1**
1	0

References and Sources on the Internet

Requests for Comments (RFCs):

- Overall RFC Index
- RFC 1918 - Address Allocation for Private Internets
- RFC 1219 - On the Assignment of Subnet Numbers
- RFC 950 - Internet standard subnetting procedure
- RFC 940 - Toward an Internet standard scheme for subnetting
- RFC 932 - Subnetwork addressing scheme
- RFC 917 - Internet subnets

Newsgroups of interest:

- comp.protocols.tcpip
- comp.protocols.tcpip.domains

Other Stuff:

- InterNIC
- Zen and the Art of the Internet
- Glossary of Internet Terms

Tutorial Search: FindTutorials.com